

Operations

OPERATIONS SECURITY (OPSEC) INSTRUCTIONS

COMPLIANCE WITH THIS INSTRUCTION IS MANDATORY. This instruction implements Air Force Policy Directive (AFPD) 10-11, *Operations Security*; Air Force Instruction 10-1101, *Operations Security*, USSOCOM Directive 530-1, *Operations Security*, DoD Directive 5205.2, *DoD Operations Security Program*, July 7, 1983; Chairman, Joint Chiefs of Staff Instruction (CJCSI) 3210.01, *Joint Information Warfare Policy*, January 2, 1996; CJCSI 3213.01, *Joint Operations Security*, May 28, 1993; and all Operations Security requirements for DoD Instruction 5000.2, *Defense Acquisition Management Policies and Procedures*, February 23, 1991 with Change 1. In that OPSEC is one of the critical pillars in C2W strategy, it also directly supports AFPD 10-7, *Command and Control Warfare (C2W)*. It provides guidance for all AFSOC personnel and supporting contractors in implementing and maintaining OPSEC programs. This instruction applies to the Air National Guard (ANG) when published in ANGIND2 and to the Air Force Reserve Command (AFRC) when published in the AFRCIND2. It describes the OPSEC process, and explores and directs the integration of the OPSEC concept into AFSOC plans, operations and support activities.

This is the initial publication of AFSOCI 10-1101. It seeks to make OPSEC more user friendly by providing as much "how to" guidance as possible. Though OPSEC implementations are unique to each situation, it follows that if a "road map" is provided for the OPSEC users, it will be used far more often, personnel will become comfortable with the process, and then, experience along with human nature will cause OPSEC practitioners to reach out to embrace the full potential of operations security. It also discusses OPSEC's direct relationship to AFPD 10-7, *Command and Control Warfare (C2W)*.

OPR: HQ AFSOC/DOS (Captain John H. Carrier)

Certified by: HQ AFSOC/DOS (Colonel Mark S. Race)

Pages: 43

Distribution: F; X

	Para
Chapter 1--INTRODUCTION	
Definition	1.1.
Characteristics of OPSEC	1.2.
Air Force Operations Security	1.3.
Chapter 2--THE OPERATIONS SECURITY PROCESS	
General	2.1.
Identification of Critical Information.....	2.2.
Threat Analysis	2.3.
Vulnerability Analysis	2.4.
Risk Assessment.....	2.5.
OPSEC Measures	2.6.
OPSEC Planning	2.7.
Writing Basic OPSEC Plans	2.8.
Coordinating Basic OPSEC Plans.....	2.9.
Planning Responsibilities of Supporting and Subordinate Organizations	2.10.

Chapter 3--AFSOC OPERATIONS SECURITY PROGRAM

Purpose	3.1.
AFSOC Operations Security	3.2.
Command Involvement	3.3.
Organization	3.4.
Funding	3.5.
Training and Education	3.6.
OPSEC Program Managers	3.7.
Evaluations	3.8.
Foreign Intelligence and Counterintelligence Support	3.9.

Page**Attachments**

1. GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS	17
2. HHQ AND SUPPORTING COMMANDS RESPONSIBILITIES AND AUTHORITIES	21
3. HQ AFSOC, UNIT AND INDIVIDUAL RESPONSIBILITIES	24
4. AFSOC STANDING CRITICAL INFORMATION LIST	28
5. OPSEC TRAINING REQUIREMENTS	29
6. AFSOC OPSEC SELF INSPECTION CHECKLIST	27
7. ANNUAL OPSEC STATUS REPORT FORMAT	32
8. FLOW DESCRIPTION FOR CONTINGENCY OPERATIONS	33
9. FLOW DESCRIPTION FOR TRAINING EXERCISES	35
10. FLOW DESCRIPTION FOR CURRENT OPERATIONS	37
11. FLOW DESCRIPTION FOR DOCTRINE, PROGRAMMING AND ACQUISITION	39
12. FLOW DESCRIPTION FOR RESOURCE BUDGETING/ALLOCATION PROCESS	41
13. CONTINUITY BOOK FORMAT	43

Chapter 1

INTRODUCTION

1.1. Definition. OPSEC is a **process** of identifying critical information and analyzing friendly actions attendant to military operations and other activities to a.) identify those actions that can be observed by potential adversaries; b.) determine indicators that could be interpreted or pieced together to derive critical information in time to be useful to an adversary; and, c.) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

1.2. Characteristics of OPSEC. The goal of OPSEC is to control information and observable actions about mission capabilities, limitations, and intentions in order to prevent or control exploitation by an adversary. Operational effectiveness is enhanced when commanders and other decision makers apply OPSEC during the earliest stages of planning. OPSEC provides a step-by-step analysis of operations and behavior, from an adversarial point of view, to determine how vulnerabilities might be exploited in time to be of use to an adversary.

1.2.1. OPSEC analysis examines the planning, preparation, execution, and post execution phases of any activity across the entire spectrum of military activity, and in any operating environment. Air Force commanders and decision makers should consider OPSEC during both mission and acquisition planning.

1.2.2. OPSEC should be closely coordinated with security disciplines (Physical Security, AFI 31-101; Information Security, AFI 31-401, and Information Protection, AFI 33-2) to ensure that all aspects of sensitive activities are protected. Potential exploitation of open sources and observable actions are a primary focus of OPSEC analysis. These sources are generally unclassified and, consequently, more difficult to control. The analysis facilitates risk management by providing decision makers with a means of directly assessing how much risk they are willing to accept.

1.3. Air Force Operations Security. The Air Force implements the OPSEC process in all functional areas. Commanders are responsible for OPSEC awareness throughout their organizations and for integrating the OPSEC process throughout appropriate mission areas.

1.3.1. OPSEC is an integrated component of Information Warfare (IW) . It provides a means of detecting and controlling an adversary's actions on our military information functions. OPSEC assists in protecting IW capabilities and intentions from adversary knowledge and attack.

1.3.2. In acquisition, research and development efforts are enhanced through reduction in compromised technology and proprietary information. Organizations that fail to implement OPSEC are more likely to unintentionally give away critical information and expose missions to increased risk.

1.3.3. OPSEC should be considered simultaneously with complementing and competing activities to obtain maximum effectiveness. Planners and decision makers should consider operational objectives, strategies, deception, psychological operations, electronic warfare, and traditional security measures as a single effort to control perception, decisions and activities of an adversary.

1.3.3.1. Complementing Activities. There are a host of other concepts, activities, procedures, disciplines, and systems that complement the positive control of information. When they are considered with OPSEC measures, as alternative methods for controlling information, flexibility and ultimately, greater security is added to operations. When OPSEC measures are planned in conjunction with

deception, psychological operations, electronic combat and other traditional security programs, synergism occurs in the C2W environment.

1.3.3.2. Competing Activities. Several factors exist that continually compete with information protection. Examples include: information releases to the media, foreign military sales, treaty provisions, business agreements and normal operating procedures.

Chapter 2

THE OPERATIONS SECURITY PROCESS

2.1. General. OPSEC analysis is accomplished through the use of a five step process. This process is the most important aspect of OPSEC. It determines how well OPSEC is being integrated into both mission planning and execution. Each application of the process represents a closed loop effort that is to be reapplied as activities, events, situations, and operations change. *NOTE:* The same process used to plan an operation is also the one used to survey or, to evaluate it. In fact the process can be applied to *any* situation in which there is competition.

2.1.1. The five steps of the OPSEC process are:

- 2.1.1.1. Identification of Critical Information (and its indicators).
- 2.1.1.2. Analysis of Threats.
- 2.1.1.3. Analysis of Vulnerabilities.
- 2.1.1.4. Assessment of Risk.
- 2.1.1.5. Application of Appropriate Countermeasures.

2.1.2. OPSEC will be applied to the following five areas, plus other activities as deemed appropriate. A flow description of each area is at Attachments 8-12:

- 2.1.2.1. Contingency operations and planning
- 2.1.2.2. Training exercises
- 2.1.2.3. Current operations to include SORTS and deployment reporting
- 2.1.2.4. Force and doctrine development, and defense acquisition system process
- 2.1.2.5. Resource programming/allocation process

2.2. Identification of Critical Information. Critical information is information about friendly (U.S., allied, and/or coalition) activities, intentions, capabilities or limitations an adversary needs in order to gain a military, political, diplomatic, or technological advantage. Such information, if released to an adversary prematurely, may prevent or forestall mission accomplishment, reduce mission effectiveness, or cause an unacceptable loss of lives and/or damage to friendly resources. Critical information may also be derived from bits and pieces of related information (indicators) that are almost always perceptible to the trained eye. Examples of indicators are provided, with the AFSOC standing critical information list, at Attachment 4.

2.2.1. Those individuals responsible for the development and execution of the operation itself best identify critical information. They possess the intimate familiarity necessary to properly apply the OPSEC concept to the task at hand.

2.2.2. Mission critical information is to be identified by commanders and planners at the earliest possible time, usually during the conceptual planning phase of an activity. Subordinate commanders and supporting organizations will then be notified to control not only the identified critical information, but also the *indicators* of that critical information, which can also be collected and exploited by potential adversaries.

2.2.3. A list of critical information will be developed and appropriately revised to reflect changing situations. Critical information is usually only critical for a prescribed period of time and the need to

control or protect specific items of information will most likely change as an operation progresses and/or as the adversarial threat changes.

2.2.4. Directors and units will identify contractor requirements to control and protect certain critical information. Contractors will continue to control such information until notified, in writing, that the need for OPSEC measures no longer exists.

2.3. Threat Analysis. OPSEC planners and commanders must use current threat information to develop appropriate OPSEC measures. This information is available from authorized USAF and DoD intelligence and counterintelligence organizations. An OPSEC threat analysis includes identifying adversaries and their capabilities, limitations, and intentions to collect, analyze, and use critical information and OPSEC indicators against friendly forces. This analysis must be tailored to the particular operation, test, project, geographic region, or facility.

2.3.1. The Air Force Office of Special Investigations (AFOSI) produces counterintelligence studies and analyzes multidiscipline intelligence threats posed to US Air Force and DoD programs and resources by foreign intelligence services. Contact Detachment 309 at Hurlburt Field, or your servicing AFOSI detachment to request counterintelligence studies or multidiscipline counterintelligence.

2.3.2. To request foreign intelligence threat information, call the Air Force Information Warfare Center's Operations Support Central (AFIWC/OSC) at DSN 969-2191/2152 for 24-hour support. If they do not have the information you need, they will most likely be able to point you in the right direction.

2.4. Vulnerability Analysis. Two conditions must be present for an OPSEC vulnerability to exist: 1) There is a weakness that could reveal critical information, and 2) there is an adversary with *both* the *intent* and the *capability* to exploit that weakness (i.e., a threat). Efforts must be undertaken to identify an organization's potential vulnerabilities. Once identified, these vulnerabilities must be either outright denied or proactively controlled.

2.4.1. At times, it may not be cost-effective or even possible to alter the source of an OPSEC indicator. In that instance, it may be prudent to take a proactive approach by attempting to disrupt or confuse the adversary's ability to collect and/or properly interpret the information. Hence, OPSEC measures should also be considered as a means to control the adversary and their ultimate comprehension or use of the information when an OPSEC indicator or indicators cannot be modified.

2.5. Risk Assessment. Risk assessment involves an informed estimate of an adversary's capability to exploit a friendly weakness; the potential effects such exploitation will have on an operation, activity, or weapon system and a cost-benefit analysis of actions contemplated to counter the vulnerability. Risks are reduced or eliminated by employing OPSEC measures to control the availability of information to the adversary.

2.5.1. OPSEC program managers, in concert with other planners, and with the assistance of intelligence and counterintelligence organizations, will accomplish risk assessments and provide recommendations to commanders (the senior decision makers). Commanders, who are ultimately responsible for mission success, must decide whether or not to employ OPSEC measures.

2.6. OPSEC Measures. OPSEC measures are employed to counter or eliminate vulnerabilities that point to or divulge critical information. They help to deny critical information by controlling the raw data adversaries use to make decisions, thereby limiting their effectiveness and possibly their credibility.

OPSEC measures also enhance friendly capabilities by increasing the potential for surprise and effectiveness of friendly military forces and weapon systems.

2.6.1. OPSEC measures can be used to eliminate the source of indicators or vulnerabilities of friendly actions to exploitation by adversary intelligence systems through action control. Specifically, select what actions to undertake; decide whether or not to execute actions necessary to accomplish tasks. When it is impossible or impractical to use action control procedures, countermeasures may be employed to disrupt effective adversary information gathering or prevent their recognition of indicators when collected materials are processed. Use unit system designs and procedures to create diversions, camouflage, conceal, jam, or use force against adversary information gathering and processing capabilities. Another method is to employ counter-analysis. The objective of counter-analysis is to prevent accurate interpretation of indicators during adversary analysis of collected materials. This is done by confusing the adversary analyst through deception techniques such as covers. Finally, protective measures are methods to create closed information systems to prevent adversaries from gaining access to information and resources. Examples include cryptologic systems and standardized security procedures.

2.6.2. At the very heart of the OPSEC concept is risk management by commanders and senior decision makers. OPSEC measures must preserve the effectiveness of friendly military capabilities while controlling the adversarial exploitation of critical information to the maximum extent possible. Determining the delicate balance between OPSEC measures and operational needs is always the commander's decision. Commanders must decide whether organizational activities, which yield OPSEC indicators, jeopardize the attainment of friendly initiative, surprise, or superiority and, if so, to what degree?

2.6.3. OPSEC measures that control critical information and OPSEC indicators must be developed as operations are planned to complement mission objectives and strategies. Individuals who are most familiar with the operation should develop and recommend OPSEC measures. However, an office of primary responsibility within the Plans and/or Operations should centrally supervise OPSEC measures to ensure their purpose is consistent with mission needs.

2.6.4. Sometimes it may not be cost-effective or possible to alter the source of an OPSEC indicator. In these circumstances, attempts to disrupt or confuse the adversary's ability to collect and/or properly interpret the information may be required. OPSEC measures should be considered as a means to influence the adversary and their ultimate comprehension or use of the information when an indicator cannot be modified. Measures to control critical information and OPSEC indicators involve a full range of possibilities that are limited only by the user's imagination.

2.6.5. AFSOC and supporting organizations will develop and execute OPSEC measures that:

2.6.5.1. Are consistent with operational mission needs

2.6.5.2. Deny (by controlling) critical information, OPSEC indicators, and the sources of such information to prevent degrading the effectiveness of friendly plans, forces, weapon systems, defense systems, and command and control

2.6.5.3. Degrade the effectiveness of adversary decisions, command and control, and weapon systems to limit the effectiveness of adversary forces

2.7. OPSEC Planning. Effective implementation of the OPSEC concept requires deliberate planning. Such planning ensures that OPSEC is implemented in a pro-active manner and is integrated into all

operations and support activities by design. Equally important, it also ensures that critical information, OPSEC indicators, and OPSEC measures are properly coordinated with all participating organizations.

2.7.1. All AFSOC organizations conducting or supporting operational missions must develop OPSEC into their plans to ensure mission critical information, information sources, OPSEC indicators, foreign intelligence threats, and the adversary's use of information are understood and "controlled" according to the unique circumstances of each mission. OPSEC planning must focus on mission needs, provide guidance and coordination, and ensure information is consistently controlled across organizational lines. Once critical information is determined and coordinated, participating organizations can determine OPSEC indicators (of that critical information) and OPSEC measures, as necessary.

2.7.2. As organizational activities begin, they should be monitored to assess the need to adjust for changing mission needs as well as to the adversary's changing capabilities and intentions. During the Mission Area Plan (MAP) and acquisition process, operational planners must work directly with program personnel to determine critical information and the general requirements for controlling information.

2.7.3. Continuous OPSEC planning ensures flexibility and continuous improvements during changing missions and threats. Cost-effectiveness and common sense dictates that we only protect critical information from an adversary for as long as it is critical to mission effectiveness.

2.7.4. OPSEC planning is the joint responsibility of the OPSEC program manager (as the facilitator), other planners (as appropriate for the mission at hand), foreign intelligence and counterintelligence organizations, and commanders. In circumstances involving particularly complex operations, commanders may find it useful to create dedicated OPSEC planning groups.

2.7.5. Attachments 8-12 contain flow descriptions for applying OPSEC to the five required areas. These decision matrices are guides to help organize your efforts. Do not, however, let them be a substitute for common sense and good judgment.

2.8. Writing Basic OPSEC Plans. Basic OPSEC plans must be developed during the very conception of operations and acquisition planning and must include the following items. [NOTE: References to developing OPSEC plans do not necessarily mean the creation of a separate, single OPSEC plan. For our purposes, the term "OPSEC plan" can mean a separate plan, an annex to a larger plan, or simply the overall integration of OPSEC into and throughout a plan.]

2.8.1. Direction for participating organizations to control critical information, OPSEC indicators, and the sources of such information to prevent its exploitation. NOTE: Specific sources of critical information (and any associated OPSEC indicators) may be different for each functional activity in an organization.

2.8.2. Critical information and OPSEC vulnerabilities applicable to mission at hand. Critical information must be identified during the conceptual phase of planning. OPSEC planners must consider adversarial objectives, the knowledge they need to effectively plan against friendly forces, and their capability to gain such information.

2.8.3. Direction to continuously monitor and review friendly activities for the express purpose of identifying changing parameters as the operation matures. Changes must be plugged back into the OPSEC equation and recommendations made to either modify existing OPSEC measures or create new ones.

2.8.4. Intelligence Threat Information. Air Force foreign intelligence and counterintelligence organizations will provide this information and should include the following:

2.8.4.1. Adversarial intelligence collection capabilities, presence and intentions. These factors must be continually assessed throughout the duration of each operation.

2.8.4.2. Critical Information. When critical information pertinent to the existing or planned situation are known, they will be listed.

2.8.4.3. Probable adversary knowledge. OPSEC planners must consider the knowledge an adversary already has about a situation (from general knowledge, open source information, or from what they will know when the plan is implemented) to determine OPSEC vulnerabilities. Specific OPSEC measures will then be planned to address additional information that is considered to be of intelligence value to an adversary. OPSEC surveys are an additional method of determining probable adversary knowledge.

2.8.5. Detectable Activities and OPSEC Indicators. OPSEC plans must address detectable sources of critical information and OPSEC indicators that will not be protected by closed information systems (such as the STU III or the classification marking and storage program). Examples of detectable activities include emissions or reflections of energy; observable personnel or material actions; public releases, unsecured communication, documents, procedures, arrangements with foreign countries, and compliance with treaties. The relationships of OPSEC indicators that match the detectable activities will also be listed. These indicators occur in all functional areas.

2.8.6. OPSEC Measures. Once identified, organizations will control or eliminate OPSEC indicators where possible. OPSEC measures must be planned and executed in a proactive manner and considered for both offensive and defensive operations and support activities. When OPSEC indicators cannot be avoided, cover and deception will be used to confuse the adversary and their analysis of the information. Measures might also be developed to control the threat.

2.8.7. Documentation. The results of OPSEC planning will be documented in ANNEX L of supporting plans IAW JCS PUB 5-03.1 for operations plans and in the corresponding paragraph of OPORDs to subordinate units. Free form can be used in other applications. Ensure HQ AFSOC OPSEC program manager receives a copy of any OPSEC planning documentation.

2.9. Coordinating Basic OPSEC Plans. Basic OPSEC plans must be appropriately coordinated within supported and supporting organizations to ensure critical information is consistently controlled across and throughout the infrastructure spectrum. Since exploitable information resides in numerous sources in most organizations and activities, OPSEC plans must be developed and implemented--or at the very least, complied with--by all functional areas. Many times, the sources of information are unique to the organization's function and may only be known to the individuals of that organization. Therefore, each organization must at least identify OPSEC indicators and then develop and execute OPSEC measures that eliminate or control the exploitation of information.

2.10. Planning Responsibilities of Supporting and Subordinate Organizations. Subordinate and supporting organizations must develop their own OPSEC plans to support basic OPSEC plans--plans that focus on those mission needs that are defined in the basic guidance. In addition, supporting organizations must participate in the OPSEC measures required by the basic guidance.

2.10.1. OPSEC planning guidance must be developed by those most familiar with the operational aspects of a particular activity at hand and then shared with people who have a valid need-to-know.

2.10.2. Each organization will ensure the OPSEC concept and any known OPSEC measures are applied consistently--across the board--in all plans, activities, processes, and procedures that involve either critical information or indicators of that critical information.

Chapter 3

AFSOC OPERATIONS SECURITY PROGRAM

3.1. Purpose. To provide AFSOC decision makers at all levels with a means of promoting understanding and awareness in the integration and application of OPSEC. The AFSOC OPSEC Program provides the Headquarters and all subordinate units with standardized policy to facilitate an effective OPSEC program.

3.2. AFSOC Operations Security. AFSOC implements the OPSEC process in all functional areas. The command's goal is to develop and maintain a standing program that will prevent an adversary's timely exploitation of critical friendly information. This goal supports AFSOC's number one command goal, to "enhance combat readiness" through improved survivability. In order to achieve this goal, we must:

3.2.1. Develop an effective plan, which integrates the OPSEC process across the entire spectrum of AFSOC's daily activity and applies the analysis process when critical information is identified.

3.2.2. Continually assess current operations, OPLAN/CONPLAN preparation, training activities, force development plans and programs, Mission Area Plans (MAPs) and Weapon System Roadmaps.

3.2.3. Incorporate traditional security disciplines and staff functions as integral players in OPSEC planning and execution.

3.2.4. Integrate OPSEC into the command's Information Operations/Warfare program.

3.2.5. Conduct an aggressive OPSEC training program.

3.3. Command Involvement. Commanders are responsible for the appropriate use of the OPSEC concept and must ensure OPSEC guidance is developed as early as possible in the planning and coordination process. Commanders may delegate authority for the management of the OPSEC program and the execution of OPSEC measures, but must personally make the key decisions with respect to the implementation of OPSEC measures and provide necessary guidance to subordinates.

3.4. Organization. The AFSOC OPSEC Program organizes Headquarters AFSOC (HQ AFSOC) and all subordinate unit OPSEC programs; provides an OPSEC program manager at HQ AFSOC; integrates OPSEC into AFSOC supporting plans; and develops policy and guidance that provides for the coordination, training, education, and recognition of all unit OPSEC programs and program managers.

3.4.1. A command OPSEC program manager will be appointed by the HQ AFSOC Director of Operations (DO) to administer the overall OPSEC program. Each HQ AFSOC director will appoint an OPSEC Point of Contact (POC) who will coordinate OPSEC matters between the OPSEC organization and personnel in his/her division. 16SOW, 193SOG, 720STG, 919SOG, 18 FLTS and USAFSOS will establish OPSEC programs appropriate to policies of this publication. 352SOG, 353SOG, and other AFSOC units not OPCON to HQ AFSOC, will be provided informational copies of command OPSEC guidance. Requests for OPSEC support will be honored to the greatest extent possible.

3.4.2. Program Placement. OPSEC is an operations management program. Management of the OPSEC program requires a thorough understanding of operations objectives, activities, the planning of those activities, and the relationships that exist with respect to other activities. Only the function responsible for plans and operations can assess the value of information; only that function can decide whether to implement the more pro-active OPSEC measures (deception, psychological operations, and electronic combat) as a means of denying critical information to an adversary and positively ensure the complete

and effective implementation of OPSEC measures. Effective OPSEC is often extremely time-sensitive, by the time other functional areas become aware of the need for OPSEC measures, it is often too late. In order to ensure the operational orientation, the office of primary responsibility (POC or program manager) for the OPSEC program should be located within the Plans and/or Operations element of an organization.

3.4.3. AFSOC will establish a semi-annual OPSEC working group, consisting of AFSOC program managers and directorate POCs. The DO, or his designated representative, will chair the committee.

3.4.4. Integration. The OPSEC concept must be integrated into all organizational plans and activities. Staff elements and supporting organizations must ensure OPSEC thinking is appropriately incorporated--at the earliest possible time--into all operations plans, MAPs and Weapon System Roadmaps, CONPLANS, operations orders, exercise plans, Mission Needs Statements (MNS), Operational Requirements Documents (ORD), operating procedures, operations, exercises and other plans and activities to consistently and positively control critical information and OPSEC indicators. Due to their complementary aspects, the programs of IW/C2W, Tactical Deception (TD), and OPSEC must be fully integrated.

3.4.5. Coordination. Commanders must control critical information at all sources and at all levels. Coordination across functional and organizational lines facilitates OPSEC planning and enhances the effectiveness of OPSEC measures. In addition, commanders and/or OPSEC program managers must closely coordinate and build a rapport with foreign intelligence and counterintelligence organizations to identify potential adversaries and their intelligence collection capabilities and intentions, and to support OPSEC survey efforts.

3.5. Funding. OPSEC is a low-cost/high-output concept, which draws more on rethinking a situation than it, does requiring an additional outlay of funds or a new funding stream. Most OPSEC measures are the result of relatively simple modifications to existing plans and operations. HQ AFSOC/DO will program for and fund the HQ AFSOC OPSEC program and associated activities deemed necessary to orchestrate the AFSOC OPSEC program. Units will fund travel and expenses required to support their individual programs and training. Air Intelligence Agency/Air Force Information Warfare Center (AIA/AFIWC) will fund for and provide training aids and materials for use by OPSEC program managers throughout the growing OPSEC infrastructure.

3.6. Training and Education. The purpose of OPSEC training and education is to ensure AFSOC people understand: a.) the positive benefits of OPSEC; b.) the effects of foreign intelligence collection on mission effectiveness and c.) what AFSOC does to control the exploitation of critical information. OPSEC education and training should be continuing and ongoing throughout each Service member's period of service. Formal education and training activities should contain OPSEC as a subject of curriculum and an objective of training exercises by integrating principles of awareness, analysis application, and survey procedures.

3.6.1. The academics of AFSOC schools should promulgate the doctrinal base of OPSEC, which should include OPSEC into the formal instruction and the addition of OPSEC as ancillary information to select subjects or practical exercises. Additionally, an OPSEC analysis may be a necessary action to ensure protection of information associated with sensitive activities or curriculum of the academic institution.

3.6.2. Training activities from the joint readiness exercise (JRX) level down through the small unit tactics level, should contain OPSEC considerations and applications appropriate to training goals where tasks, conditions, and standards are applied. Real-world sensitivities relating to capabilities and

methodologies to which training activities are focused may also require the application of OPSEC protective measures.

3.6.3. OPSEC considerations will be included in the evaluation of units on training tests, readiness inspections and field exercises.

3.6.4. All training will be conducted in a manner that precludes compromise of operational plans and procedures.

3.6.5. Unit OPSEC Training. The purpose of unit OPSEC training is to ensure all AFSOC personnel understand the foreign intelligence threat as it relates to their mission; critical information for the missions they support; job specific OPSEC indicators; and the OPSEC measures they will execute.

3.6.5.1. Initial training will be developed and presented to newly assigned personnel within 90 days after arrival for duty. As a minimum, it must include:

3.6.5.1.1. Duty related mission critical information and OPSEC indicators

3.6.5.1.2. Foreign intelligence threat to missions supported and conducted

3.6.5.1.3. Individual responsibilities

3.6.5.2. At the direction of the on scene commander, an OPSEC orientation will be presented to personnel who are deployed in support of a contingency operation, or to an unfamiliar OCONUS location.

3.6.5.3. Annual Training. Once per year every individual, OPCODE to AFSOC, must receive OPSEC training which covers the items in Attachment 5. OPSEC program managers and POCs are responsible for annual training of their personnel. To assist in providing a standardized product where applicable, the HQ AFSOC OPSEC program manager will provide training material to the trainers. Developing and briefing directorate or unit specific items are the responsibility of the individual trainers. An Air Force SafeWare computer-based training OPSEC module covering all the categories in Attachment 5 will be accessible to all AFSOC personnel. The decision to use the AFSOC training material rests with the OPSEC instructor, however all the categories shown at Attachment 5 must be covered.

3.6.6. OPSEC Program Manager Training. Advanced job-specific training is required for those individuals who are either designated as unit OPSEC program managers, directorate POCs, or who perform *formal* OPSEC surveys. Such OPSEC training must be current, recurring, and received within 90 days of initial assignment, if at all possible. Training is available through AFIWC/OSW, the National Cryptological School, and USSOCOM J3-OS. HQ AFSOC OPSEC program manager is the POC for coordinating training and will work with the formal trainers to conduct one class per year at Hurlburt Field FL.

3.7. OPSEC Program Managers. HQ AFSOC will assign a full-time program manager. All other units are *encouraged* to assign full time managers, as appropriate, depending upon their operational relationships. Because of the similarity of process and indefinite boundary between OPSEC and Tactical Deception (TD), AFSOC units should establish mutually supporting programs. When possible, OPSEC and TD officers should be each other's alternate or the same individual. If OPSEC is assigned as an additional responsibility, it will either be combined with TD or it will be the only additional duty assigned that person. To be effective, the program manager must be cleared for access to TS-SCI information in order to properly "facilitate" the OPSEC planning process. In the acquisition

environment, the OPSEC program manager will work directly with program directors to ensure OPSEC principles are integrated and applied throughout the life cycle of all programs.

3.7.1. OPSEC program managers are responsible for advising commanders on OPSEC-related matters, facilitating OPSEC implementation, and managing the organization's OPSEC program.

3.7.2. OPSEC program managers must participate in and "facilitate" the conception phase of mission planning to help develop command guidance and to assist other planners in developing and integrating OPSEC "thinking" into their plans and programs.

3.7.3. OPSEC program managers must be familiar with higher echelon direction, goals, objectives, strategies, activities and the personnel who participate in those activities to understand what information is critical and how it applies to the organization's primary mission. The OPSEC program manager can then be invaluable when helping to develop and recommend OPSEC measures that will have a realistic and positive effect on the outcome of the mission.

3.7.4. OPSEC program managers will interface with supported and supporting units and offices to ensure continuity of effort and complementary OPSEC measures.

3.7.5. OPSEC program managers must be thoroughly familiar with and supportive of the C2W concept. As required, they must work to integrate OPSEC with the other four activities that support the C2W Strategy (Military Deception, Psychological Operations (PSYOP), Electronic Warfare (EW), and physical destruction). Only then can the synergism be realized that results from the integrated employment of these five "pillars" of C2W. Other duties of OPSEC program managers are listed at Attachment 3.

3.8 Evaluations. There are several methods used to evaluate OPSEC programs and the effectiveness of OPSEC measures. These include OPSEC Surveys, Telecommunications Monitoring, OPSEC Appraisals and Status Reports, and Inspector General Evaluations

3.8.1. OPSEC Surveys. OPSEC surveys help determine how well an organization's critical information is being denied to adversaries. The survey is an analysis of friendly activities and foreign capabilities to determine what information an adversary may gain about our warfighting capabilities, limitations and intentions; how that information can be collected and used against friendly forces; and concludes by recommending corrective OPSEC measures, as appropriate. They are most effective when approached from an adversarial point-of-view. There is literally no limit as to what discipline, tool, or specialization can be called upon to support a thorough OPSEC Survey. In a properly supported survey, you should have whatever expertise you need to provide the commander a complete and accurate picture. Survey results and recommendations are proprietary information to the surveyed organization's commander. Guidance for conducting OPSEC surveys can be found in AFMAN 10-1106, AIA/OSW OPERATIONS SECURITY ASSESSMENT HANDBOOK, and JCS PUB 3-54.

3.8.1.1. Commanders will consider accomplishing an OPSEC survey whenever their missions change, a new adversary is identified, or an adversary's intelligence gathering capabilities and/or intentions change. OPSEC surveys will also be considered to increase the potential effectiveness of a sensitive on-going mission. Commanders should evaluate the costs and benefits of an OPSEC survey by assessing the value of the mission against the effect that foreign intelligence exploitation would have on mission success.

3.8.1.2. The commander responsible for the operation or activity surveyed must ensure the identification of critical information. Without that basis, OPSEC vulnerabilities cannot be determined.

3.8.1.3. There are two (2) ways to do an OPSEC survey:

3.8.1.3.1. AFIWC is responsible for conducting professional-level OPSEC surveys with an in-depth, multi-disciplined approach. Unit commanders may request OPSEC surveys through HQ AFSOC/DOS. HQ AFSOC OPSEC program manager will request no less than one survey per year from AFIWC/OSW.

3.8.1.3.2. Commanders are also encouraged to build their own ad hoc OPSEC survey team(s) from within available resources--facilitated by the OPSEC program manager--to effect, on an as needed basis, a low-cost, in-house survey. An alternative benefit to be gained here is the expansion of local awareness by intimately exposing key personnel to the benefits of the OPSEC concept.

NOTE: OPSEC surveys are but a "snapshot in time". They effectively describe your OPSEC posture at the time they are performed. In essence, the survey tells you how well you are incorporating the OPSEC concept into whatever activity is being surveyed.

3.8.2. Telecommunications Monitoring. The express purpose of telecommunications monitoring is to provide feedback to the commander's OPSEC program. Telecommunications monitoring involves the electronic monitoring and analysis of unsecured phones, faxes, radios, and computers to estimate an organization's OPSEC posture. Telecommunications monitoring is also an effective tool, which may well be used by itself--apart from a survey--to provide a useful OPSEC product. 25IS at Hurlburt Field and AFIWC conduct telecommunications monitoring, and can be scheduled through the HQ AFSOC OPSEC program manager.

3.8.3. OPSEC Appraisals and Status Reports. OPSEC program managers and directorate POCs will accomplish an annual appraisal through the use of the self-inspection checklist at Attachment 6. Unit program managers will submit a report IAW Attachment 7 to COMAFSOC, Attention HQ AFSOC OPSEC program manager, NLT 15 Oct. HQ AFSOC OPSEC program manager will send the command annual OPSEC report to USCINCSOC, Attention SOJ3-OS and AFIWC/OSW NLT 1 Nov. Comments and/or concerns relating to the quality of counterintelligence support being received in the field will be forwarded directly to AFOSI Investigative Operations Center for review, evaluation, and action as needed (with an information copy to HQ USAF/XOOP).

3.8.4. Inspector General Evaluations. The extent to which Air Force components maintain their OPSEC programs will be assessed during Inspectors General evaluations IAW AFSOCI 90-202. Areas of interest include commanders' involvement and integration of OPSEC into unit plans and operating procedures, Weapon System Roadmaps, and training programs.

3.9. Foreign Intelligence and Counterintelligence Support. Commanders require the most accurate and complete threat information available to properly implement the OPSEC process. As such, no direction stipulated herein is meant to restrict a commander's access to any one source for threat information. In fact, commanders are encouraged to seek the most accurate and focused information available to augment their free-form OPSEC thinking. HQ AFSOC/IN and the AFOSI Detachment 309 will plan and coordinate operational requirements and associated threat assessments with other DoD foreign intelligence and counterintelligence organizations to ensure the availability of current, timely,

and accurate threat information for commanders and customers at Hurlburt Field FL or in the field. Units assigned to other bases will use their OSI.

STEPHEN R. CONNELLY
Col, USAF
Director, Operations

Distribution X:

USSOCOM (1)
HQ USAF (1)
USASOC (1)
NAVSPECWARCOM (1)
JSOC (1)

Attachment 1**GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS*****References***

DOD Directive 5205.2, 7 July 1983, "DOD Operations Security (OPSEC) Program." (Undated Revision in Draft)

CJCS INST 3213.01, 28 May 1993, "Joint Operations Security."

Joint Pub 3-54, 29 August 1991, "Joint Doctrine for Operations Security."

JCS OPSEC SURVEY GUIDE

USSOCOM Directive 530-1, 1 July 1993, "Plans and Operations, Operations Security."

USSOCOM OPSEC Guide

Air Force Manual 10-401, Chapter 24, "Operations Security Planning"

Air Force Policy Directive 10-11, 17 December 1996, "Operations Security".

Air Force Information Warfare Center, 1 June 1994, "OPSEC Assessment Handbook."

AFSOC Instruction 10-1101, 1 February 1997. "Operations Security Instructions."

IOSS Monograph Series, April 1990, "OPSEC Program Development Procedural Guide."

IOSS Monograph Series, July 1991, "OPSEC Program Evaluation."

IOSS Monograph Series, October 1991, "OPSEC Planning--A Management Tool--."

IOSS Monograph Series, October 1991, "Treaty Inspections OPSEC Survey Guide."

National Cryptological School Publication, March 1991, "A Guide to Performing OPSEC Assessments."

National Cryptological School, "OPSEC Practitioner Guide"

Dr. Peoples, "Are You Safeguarding the Crown Jewels? Determining Critical and Sensitive Information."

Abbreviations and Acronyms

AETC	Air Education and Training Command
AFIWC	Air Force Information Warfare Center
AFOSI	Air Force Office of Special Investigations
AFSOC	Air Force Special Operations Command
AIA	Air Intelligence Agency
C2W	Command and Control Warfare
C3	Command, Control and Communications
CI	Critical Information
CIL	Critical Information List
CISO	Counterintelligence Staff Officer
CM	Countermeasure
COMAFSOC	Commander, AFSOC
COMSEC	Communications Security
CONOPS	Concept of Operations
CONPLAN	Concept Plan
DO	Director of Operations
EW	Electronic Warfare
EXPLAN	Execution Plan
FLTS	Flight Test Squadron
FRAGORD	Fragmentation Order
HHQ	Higher Headquarters
HUMINT	Human Intelligence

IAW	In Accordance With
IMINT	Imagery Intelligence
IS	Intelligence Squadron
IW	Information Warfare
JCS	Joint Chiefs of Staff
MAP	Mission Area Plan
MDCI	Multidiscipline Counterintelligence
MNS	Mission Need Statement
OPCON	Operational Control
OPLAN	Operation Plan
OPORD	Operation Order
OPSEC	Operations Security
ORD	Operational Requirements Document
POC	Point of Contact
PSYOP	Psychological Operations
SIGINT	Signals Intelligence
SOG	Special Operations Group
SOP	Standard Operating Procedures
SOW	Special Operations Wing
STG	Special Tactics Group
TD	Tactical Deception
USAFSOS	United States Air Force Special Operations School
USCINCSOC	Commander-In-Chief, United States Special Operations Command
USSOCOM	United States Special Operations Command

Terms

Capability. The ability to execute a specified course of action. (A capability may or may not be accompanied by an intention) (Joint Pub 1-02). *NOTE:* When considering vulnerabilities, a capability requires the physical and mental attributes and sufficient time required for performance.

Closed Information Systems. A group of interacting or interdependent procedures and devices acting together to provide information to its users and totally prohibit access to outsiders. It provides its users strict secrecy, prevents information compromise and completely protects the integrity and availability of the information within the system. Examples are secure telephone systems, isolated computer stations, and activities within a building that cannot be detected or observed from the outside.

Critical Information. Specific facts about friendly intentions, capabilities, limitations, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment.

Information Operations/Warfare. The integrated use of Operations Security (OPSEC), Military Deception, Psychological Operations (PSYOP), Electronic Warfare (EW), and Physical Destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary command and control capabilities against such actions. Information Operations/Warfare applies across the operational continuum and all levels of conflict..

Counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers,

organizations, or persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs. (Executive Order 12333)

Exploitation. 1. Taking full advantage of success in battle and following up initial gains. 2. Taking full advantage of any information that has come to hand for tactical or strategic purposes. 3. An offensive operation that usually follows a successful attack and is designed to disorganize the enemy in depth. (Joint Pub 1-02)

Foreign Intelligence. Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence (except for information on international terrorist activities).

Intelligence System. Any formal or informal system to manage data gathering, to obtain and process the data, to interpret the data, and to provide reasoned judgments to decision makers as a basis for action. The term is not limited to intelligence organizations or services but includes any system, in all its parts, that accomplishes the listed tasks. (Joint Pub 1-02)

Intention. An aim or design (as distinct from capability) to execute a specified course of action. (Joint Pub 1-02)

Military Deception. Actions executed to mislead foreign decision makers, causing them to derive and accept desired appreciations of military capabilities, intentions, operations, or other activities that evoke foreign actions that contribute to the originator's objectives. There are three categories of military deception: strategic, tactical, and Department/Service (see Joint Pub 1-02).

Multidiscipline Counterintelligence (MDCI) Threat Assessment. All-source (HUMINT, SIGINT, and IMINT) analysis of threats to a specific activity, location, operation, project, weapons or other system, deployment, or exercise.

Open Information Systems. Any information system or activity which may be accessed or observed by personnel outside of the system and provides information by open sources or OPSEC indicators. Open information systems use open source information or provide OPSEC indicators that may be observed by adversaries. Open information systems may also be influenced, jammed, interrupted, or exploited by adversaries and adversarial weapon systems. Examples are non-secure telephone systems, computer systems connected to outside lines, and non-secure radio systems.

OPSEC Appraisal. An internal evaluation or assessment of the OPSEC program, usually by the OPSEC program manager, to determine the vitality and credibility of his own program. For example: Are the components of the program in place?; have critical information and OPSEC indicators been identified and coordinated?; are necessary personnel apprised of intelligence collection methods?; etc.

OPSEC Indicator. Friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information. (Joint Pub 1-02)

OPSEC Measures. Methods and means to reduce or eliminate OPSEC vulnerabilities by controlling both critical information and the OPSEC indicators of that critical information. The following categories apply:

Action Control. Methods to eliminate or prevent detection of OPSEC indicators. Examples are:

adjusting schedules and activities and delaying information releases. First, plan activities necessary to conduct and support an operation; then, control the conduct (timing, place, etc.) of those activities to eliminate or substantially reduce OPSEC indicators.

Countermeasures. Methods to disrupt adversary information gathering sensors and data links, or preventing an adversary from obtaining, detecting or recognizing OPSEC indicators. Examples are jamming, interference, diversions and force. The objective is to disrupt effective adversary information gathering, processing, analysis, and distribution. Use units, system designs, and procedures to create diversions, camouflage, concealment, jamming, threats, police powers, and force against adversary information gathering, processing, and distribution capabilities.

Counteranalysis. Methods to affect the observation and/or interpretation of adversary intelligence analysts. Examples are military deceptions and covers. The objective is to prevent accurate interpretations of OPSEC indicators during adversary data analysis. This is done by confusing the adversary analyst through deception techniques.

Protective Measures. Methods to create closed information systems to prevent adversaries from gaining access to information and resources. Examples include cryptologic systems and standardized security procedures.

OPSEC Survey. The formal evaluation of a function, operation, activity, facility, project, or program designed to identify OPSEC vulnerabilities and provide recommendations to reduce or eliminate them. OPSEC surveys are characterized by the establishment of a dedicated survey team; use of the OPSEC process; the analysis of all sources of information; the use of a multi-discipline approach and an adversarial viewpoint to assess the effectiveness of OPSEC measures; and the preparation of a formal report.

OPSEC Vulnerability. A condition in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision making. (Joint Pub 1-02)

Psychological Operations (PSYOP). Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. (Joint Pub 1-02)

Vulnerability. 1. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. 2. The characteristics of a system which cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment. (Joint Pub 1-02)

Weapon System. A combination of one or more weapons with all related equipment, materials, services, personnel and means of delivery and deployment (if applicable) required for self-sufficiency. (Joint Pub 1-02)

Attachment 2**HIGHER HEADQUARTERS AND SUPPORTING COMMAND
RESPONSIBILITIES AND AUTHORITIES****A2.1. Headquarters, United States Air Force (HQ USAF) Responsibilities (from AFI 10-1101).**

The Deputy Chief of Staff for Plans and Operations (HQ USAF/XO) is the office of primary responsibility for the Air Force OPSEC program.

A2.1.1. HQ USAF/XO, through the Technical Plans Division (HQ USAF/XOOP), will:

A2.1.1.1. Develop OPSEC doctrine, policies, plans, and procedures consistent with joint and DoD OPSEC guidance.

A2.1.1.2. Designate an overall Air Force OPSEC program manager.

A2.1.1.3. Provide to J-3, Joint Staff, Attn: J-33/STOD/TSB, copies of all current Service OPSEC program directives and/or policy implementation documents.

A2.1.1.4. Support the National and DoD OPSEC programs as necessary.

A2.1.1.5. Provide management and annual review of the Air Force OPSEC program .

A2.1.1.6. Recommend to the Deputy Under Secretary of Defense (Policy) for Policy Support changes to policies, procedures and practices of the DoD OPSEC program .

A2.1.1.7. Utilize OPSEC training, advice, and services provided by the National Security Agency (NSA) and the Interagency OPSEC Support Staff (IOSS) when appropriate.

A2.1.2. **HQ USAF/IN** will, upon request from the commander concerned, provide Air Force units and supporting organizations with current and mission specific foreign intelligence threat information. Threat information will identify current and potential adversaries and include foreign intelligence capabilities, intentions, resources, doctrine and state-of-the-art collection methods.

A2.1.3. **HQ AFOSI** will, upon request from the commander concerned, provide Air Force units with current mission specific counterintelligence and MDCI threat assessment information.

A2.2. HQ USSOCOM Responsibilities (from USSOCOM D 530-1). Organize, budget and staff to meet the OPSEC requirements of CJCS MOP 29 and objectives in this publication. As a minimum, an OPSEC Steering Committee and a Command OPSEC officer will be identified with the following listed duties and responsibilities:

A2.2.1. **HQ USSOCOM SOJ3** will:

A2.2.1.1. Exercise primary staff responsibility for the USSOCOM OPSEC program.

A2.2.1.2. Provide for the integration of OPSEC into the curriculum/objectives of education/training activities.

A2.2.1.3. Chair the USSOCOM OPSEC committee.

A2.2.2. **HQ USSOCOM Steering Committee** will:

A2.2.2.1. Meet quarterly or at the direction of the chairman to steer the USSOCOM OPSEC program.

A2.2.2.2. Recommend USSOCOM OPSEC policy.

A2.2.2.3. Nominate ongoing headquarters activities and operations for OPSEC surveys.

A2.2.2.4. Monitor OPSEC effectiveness of HQ USSOCOM, subordinate commands and contractual activities.

A2.2.2.5. Direct OPSEC awareness training as may be required.

A2.2.2.6. Assist with training of directorate OPSEC action officers to ensure support of goals and objectives outlined in this publication.

A2.2.2.7. Integrate staff functions and traditional security programs into a mutually supporting relationship with the USSOCOM OPSEC program.

A2.2.3. HQ USSOCOM Command OPSEC Officer will:

A2.2.3.1. Maintain liaison with other agencies, activities, and commands for the purposes of coordination, training information, and operational support.

A2.2.3.2. Represent USCINCSOC at OPSEC meetings and conferences.

A2.2.3.3. Administer the functions of the OPSEC Committee as directed by the Operations Director, J3.

A2.2.3.4. Conduct the command OPSEC review program consisting of; an annual OPSEC conference, necessary actions relative to submissions of component commands annual OPSEC report, and annual command visits to component commands and other selected activities to ensure coordination of OPSEC actions and issues.

A2.2.3.5. Submit annual OPSEC program reports as required by CJCS MOP 29.

A2.2.3.6. Assist accomplishment of surveys and assessments

A2.2.3.7. Assist with acquisition of special technical support for assessments and surveys as may be required by HQ USSOCOM and component commands.

A2.2.3.8. Store and maintain command OPSEC-related information.

A2.2.4. **HQ USSOCOM Counterintelligence Staff Officer (CISO)** will coordinate counterintelligence (CI) requirements with the J3, establish liaison with the command OPSEC officer and ensure that a mechanism for passage of information on the adversaries' intelligence collection and sabotage capabilities is established. The CISO will assist the Operations Directorate in the conduct of OPSEC vulnerability assessments and surveys and assist component command CI activities as may be required.

A2.2.5. **HQ USSOCOM Inspector General** will conduct an independent evaluation of the OPSEC program on an annual basis, reporting the results to Commander in Chief; copy to SOJ3.

A2.3. Air Intelligence Agency/Air Force Information Warfare Center Responsibilities. Air Intelligence Agency (AIA), with the resources of Air Force Information Warfare Center (AFIWC), is tasked to provide administrative support, technical services, and assistance as required to HQ USAF/XOOS for OPSEC program development, planning, and execution. The focal point for OPSEC support and expertise within AFIWC is the Operations Support Directorate (OSW). Direct communication is authorized between OSW and the MAJCOM, FOA, DRU OPSEC program managers. Informal communication is authorized between OSW and their other Service and DoD agency counterparts for the exchange of information on OPSEC program matters.

A2.3.1. AIA/AFIWC will develop and maintain:

A2.3.1.1. The capability to accomplish thorough, professional level, multi-disciplined OPSEC surveys.

A2.3.1.2. OPSEC training aids and materials to support both an active marketing plan and a MAJCOM training program to be presented by OPSEC program managers in the field.

A2.3.1.3. A recurring, in-depth training course for OPSEC program managers and other personnel who perform OPSEC surveys.

A2.3.2. AIA/AFIWC will also make available to all Air Force units and supporting organizations current mission specific, foreign intelligence threat information. Threat information will identify current and potential adversaries and include foreign intelligence capabilities, intentions, resources, doctrine and state-of-the-art intelligence collection methods.

A2.3.3. Foreign Intelligence. The Air Intelligence Agency (AIA) is responsible for providing foreign intelligence threat information in support of the Air Force OPSEC program. Such data includes information relating to the capabilities, intentions, and activities of *foreign powers, organizations, or persons*, but *not* including counterintelligence (*except* for information on international terrorist activities).

A2.4. Air Force Office of Special Investigations (AFOSI) Responsibilities. AFOSI is the USAF agency responsible for counterintelligence and MDCI threat assessments. They produce studies, estimates, and analyses in support of the OPSEC program. Such data includes information relating to the capabilities, intentions, resources, doctrine, and collection methods of *foreign intelligence services* or *international terrorist activities*. In addition, AFOSI will support OPSEC program managers and commanders with OPSEC survey support, planning and training assistance, and a complete range of studies, reports, and analytical products. OSI Detachment commanders will assist their local commanders with access, as necessary, to threat information from sources outside the Air Force.

A2.5. Air Education and Training Command (AETC) Responsibilities. Air Education and Training Command (AETC) will provide for a basic, but thorough, introduction of OPSEC to all new (military) Air Force members. The block of training must include, the purpose and value of the OPSEC concept, an overview of the process, and an introduction to the application of OPSEC measures. OPSEC will be presented as "this is the way we do our day-to-day business in the United States Air Force." AETC will also provide general OPSEC education, as appropriate, in all professional level courses. Professional level materials should include the purpose and use of the OPSEC concept, the process, complementing and conflicting concepts, OPSEC planning, and command responsibilities.

Attachment 3

HQ AFSOC, UNIT, AND INDIVIDUAL RESPONSIBILITIES

A3.1. Commander Responsibilities. Though the OPSEC program helps commanders to make and implement decisions, the decisions themselves are the commanders' responsibility. Commanders must understand *the risk* to the mission and then determine whether OPSEC measures, if any, are required. Commanders must make the difficult decisions that involve risks to mission effectiveness.

A3.1.1. **Commanders** at every level will:

- A3.1.1.1. Be responsible for their OPSEC program
- A3.1.1.2. Appoint an OPSEC officer and identify them to the HQ AFSOC program manager.
- A3.1.1.3. Integrate the OPSEC concept into their mission plans and activities.
- A3.1.1.4. Ensure every person under their command understands the OPSEC concept as the way in which we conduct Air Force business; the mission critical information they need to know; the job related OPSEC indicators of that information; and the OPSEC measures employed or contemplated to neutralize any OPSEC vulnerabilities.
- A3.1.1.5. Ensure OPSEC measures are appropriately developed and executed to reinforce the combat effectiveness of units, defense systems and weapon systems.
- A3.1.1.6. Centrally manage OPSEC guidance concerning critical information to ensure consistency throughout each organization and across organizational lines.
- A3.1.1.7. Be the decision maker for risk acceptance when no countermeasures are acceptable

A3.2. All Personnel will:

- A3.2.1. Attend annual OPSEC training
- A3.2.2. Practice good OPSEC
- A3.2.3. Insure OPSEC countermeasures are included when passing sensitive information
- A3.2.4. Use OPSEC POCs
- A3.2.5. Discuss OPSEC concerns with family members

A3.3. HQ AFSOC Responsibilities. Directors will appoint an OPSEC officer and identify them to the HQ AFSOC program manager.

A3.3.1. **AFSOC/DO** will:

- A3.3.1.1. Exercise primary staff responsibility for the AFSOC OPSEC program
- A3.3.1.2. Appoint a full time Command OPSEC program manager
- A3.3.1.3. Participate in vulnerability analyses for doctrine, acquisition and programming, and budgeting
- A3.3.1.4. Oversee OPSEC committee meetings

A3.3.2. **AFSOC/DOO** will:

- A3.3.2.1. Apply OPSEC to current operations and reports
- A3.3.2.1. Develop standing Critical Information List (with indicators), and countermeasures (CMs) for current operations and reports

A3.3.3. **AFSOC/DOX** will:

- A3.3.3.1. Apply OPSEC to operations plans, exercises, and tactics development
- A3.3.3.2. Develop standing Critical Information List (with indicators) and CMs for operations plans
- A3.3.3.3. Include OPSEC considerations in evaluations of training tests, readiness inspections, and field exercises
- A3.3.3.4. Develop critical information for each OPLAN, CONPLAN, or EXPLAN
- A3.3.3.5. Prepare Annex L IAW Joint Pub 5-02.2
- A3.3.3.6. Begin application of OPSEC at beginning of planning process

A3.3.4. **AFSOC/DOS** will:

- A3.3.4.1. Apply OPSEC to contingency operations and compartmented programs
- A3.3.4.2. Develop standing Critical Information List (with indicators) and CMs for contingency operations and compartmented programs

A3.3.5. **AFSOC/FM** will:

- A3.3.5.1. Apply OPSEC to resource budgeting/allocation
- A3.3.5.2. Develop standing Critical Information List (with indicators) and CMs for Financial Management and Comptroller

A3.3.6. **AFSOC/IG** will: Assess unit OPSEC programs IAW AFSOCI 90-202.

A3.3.7. **AFSOC/IN** will:

- A3.3.7.1. Monitor and conduct OCONUS threat assessments
- A3.3.7.2. Coordinate interagency support for threat information and counter measures
- A3.3.7.3. Participate in Vulnerability Analyses
- A3.3.7.4. Integrate traditional security disciplines into OPSEC program

A3.3.8. **AFSOC/LG** will:

- A3.3.8.1. Develop standing Critical Information List (with indicators) and CMs for logistics
- A3.3.8.2. Participate in Vulnerability Analyses for contingency operations, training exercises, and current operations

A3.3.9. **AFSOC/PA** will: Maintain a close working relationship with the AFSOC program manager for guidance and press releases.

A3.3.10. **AFSOC/SC** will:

- A3.3.10.1. Develop standing Critical Information List (with indicators) and CMs for communications
- A3.3.10.2. Participate in Vulnerability Analyses for contingency operations, training exercises, and current operations

A3.3.11. **AFSOC/SF** will: Integrate traditional security disciplines into OPSEC program

A3.3.12. **AFSOC/XP** will:

A3.3.12.1. Apply OPSEC to doctrine development, programming, MAPs and Weapon System Roadmap, and acquisition

A3.3.12.2. Develop standing Critical Information List (with indicators) and CMs for doctrine development, programming and acquisition.

A3.3.13. **18 FLTS** will:

A3.3.13.1. Develop standing Critical Information List (with indicators) and CMs for tactics development, and test and evaluation

A3.3.13.2. Participate in Vulnerability Analyses for test and evaluation of AFSOC systems

A3.4. PROGRAM MANAGER RESPONSIBILITIES

A3.4.1. **HQ AFSOC OPSEC Program Manager** will:

A3.4.1.1. Establish a command OPSEC program IAW AFSOCI 10-1101

A3.4.1.2. Establish and maintain command Critical Information List

A3.4.1.3. Maintain liaison with other agencies, activities, and command for the purposes of coordination, training, information, and operational support

A3.4.1.4. Represent AFSOC at OPSEC conferences and meetings

A3.4.1.5. Assist accomplishment of surveys and assessments

A3.4.1.6. Coordinate program operations and activities with USSOCOM as may be necessary to provide assistance and technical support for the AFSOC staff and subordinate units

A3.4.1.7. Develop and maintain the command OPSEC training program

A3.4.1.8. Produce and distribute to B-Staff and Unit program managers a self inspection checklist

A3.4.1.9. Maintain AFSOCI 10-1101. Provide copy to USSOCOM and HQ USAF

A3.4.1.10. Coordinate non-intelligence interagency support through USSOCOM

A3.4.1.11. Manage command survey program

A3.4.1.12. Prioritize OPSEC initiatives, surveys, and counter measure implementation

A3.4.1.13. Host semi-annual Command OPSEC Meeting

A3.4.1.14. Maintain OPSEC database

A3.4.1.15. Review sub-unit program goals and objectives for consistency

A3.4.1.16. Submit annual report to USSOCOM

A3.4.1.17. Maintain OPSEC library (publications, training material and video tapes, and after action reports).

A3.4.1.18. Inform supported organization of AFSOC/CC decision to risk exploitation

A3.4.2. **OPSEC Program Managers and AFSOC Directorate POCs** will:

A3.4.2.1. Receive advanced OPSEC training to conduct surveys and planning

A3.4.2.2. Coordinate OPSEC with supporting and contractor organizations

A3.4.2.3. Facilitate the acceptance and implementation of OPSEC throughout their organization

A3.4.2.4. Integrate the OPSEC concept into organizational plans and activities

A3.4.2.5. Advise commanders and other primary decision makers on OPSEC matters

A3.4.2.6. Coordinate on (and facilitating the development of) OPSEC plans and measures for operations, activities, and exercises

A3.4.2.7. Integrate OPSEC requirements into C2W and information warfare strategies

A3.4.2.8. Develop, maintain and market the organization's OPSEC program

A3.4.2.9. Ensure all personnel receive appropriate OPSEC training

- A3.4.2.10. Provide OPSEC program requirements for intelligence and counterintelligence support
- A3.4.2.11. Coordinate OPSEC requirements with public affairs officers
- A3.4.2.12. Develop standing Critical Information List (with Indicators) and CMs for their unit
- A3.4.2.13. Assist in determining guidelines for controlling mission critical information and sensitive activities
- A3.4.2.14. Coordinate and facilitate OPSEC surveys
- A3.4.2.15. Maintain an effective rapport with foreign intelligence and counterintelligence agencies
- A3.4.2.16. Participate in OPSEC process that relate to unit/division
- A3.4.2.17. Provide HHQ program manager with information to update OPSEC databases
- A3.4.2.18. Participate in the Semi-annual Command OPSEC Meetings
- A3.4.2.19. Report deficiencies/improvement opportunities at Semi-annual Meetings
- A3.4.2.20. Nominate activities for OPSEC surveys
- A3.4.2.21. Annually accomplish the self inspection checklist at Attachment 6
- A3.4.2.22. Maintain continuity folder IAW Attachment 13

A3.4.3. Unit OPSEC Program Managers (in addition to A3.4.2) will:

- A3.4.3.1. Establish an OPSEC program IAW AFSOCI 10-1101
- A3.4.3.2. Include OPSEC awareness in newcomer and spouse orientations
- A3.4.3.3. Prioritize OPSEC initiatives, surveys, and CM implementation
- A3.4.3.4. Conduct annual OPSEC appraisals IAW Para. 3.1.6
- A3.4.3.5. Submit annual report IAW Attachment 7
- A3.4.3.6. Maintain OPSEC library (publications, training material and video tapes, and after action reports)
- A3.4.3.7. Include OPSEC considerations in evaluations of training tests, readiness inspections, and field exercises

A3.4.4. USAFSOS OPSEC Program Manager (in addition to A3.4.2 and A3.4.3) will:

- A3.4.4.1. Evaluate courses for appropriateness of OPSEC instruction
- A3.4.4.2. Include OPSEC in formal education and training as appropriate

Attachment 4**AFSOC STANDING CRITICAL INFORMATION LIST (CIL)**

-With Some Examples of Common Indicators

NOTE: This list is NOT all inclusive. It is provided as a starting point only. When presented with a specific operation you should use the most specific information available and your imagination to produce a tailored CIL.

Concept of Operations, planned activities

- Exercise CONOPS, SOPs
- Deconfliction coordination, schedules

Rehearsals; Association with PLAN, results

- Unscheduled or dramatically changed exercise
- Rapid changes of procedures

Deception Plans

- Uncorroborated information leaks

PSYOPS Plans

- Coordination with PSYOPS Units

Trigger Events for Execution

- Speculation by associated but unofficial personnel

Timing for Deployment, Execution, Redeployment

- Support activities

Locations of Operations

- Site surveys, requests for information

C3 Architecture

- SOPs, increased COMM traffic with a unit/HHQ, COMMEXs
- Urgent requests for communications devices

Participating Organizations

- Telephone calls between units, deployed phone list

Key Personnel; Locations, Itineraries

- Schedules, protocol coordination

Vulnerabilities, Shortfalls, Limitations, Restrictions

- SITREPs, Mission Needs Statements, FCIF, and MAPs and Weapon System Roadmap

New or Improved Tactics or Capabilities

- Open source reporting,

Rules of Engagement

- Issue of specialized ammunition/weapons

Logistics; Nodes, Supply Lines

- Coordination with suppliers or users

Friendly and Threat Intelligence Capabilities, Operations

- Flight schedules, requests for information

Effectiveness of Threat Actions

- Instructions to change standard procedures

Attachment 5**OPSEC TRAINING REQUIREMENTS**

A5.1. OPSEC Training must include the following topics:

A5.1.1. Introduction to OPSEC

A5.1.1.1. What is OPSEC ?

A5.1.1.2. How does it differ from and relate to traditional security areas ?

A5.1.1.3. How does it benefit us ?

A5.1.1.4. Examples, positive and negative

A5.1.2. OPSEC program structure

A5.1.2.1. Unit OPSEC POCs**

A5.1.2.2. HHQ OPSEC POCs

A5.1.2.3. AFSOC OPSEC POCs

A5.1.2.4. USSOCOM OPSEC POCs

A5.1.2.5. USAF OPSEC POCs

A5.1.2.6. Supporting unit OPSEC POCs**

A5.1.2.7. Supported unit OPSEC POCs**

A5.1.3. Five step OPSEC process

A5.1.3.1. Identifying Critical Information and Indicators

A5.1.3.2. Threat Assessment

A5.1.3.3. Vulnerability Analysis

A5.1.3.4. Risk Assessment

A5.1.3.5. Determining and Implementing Countermeasures (CMs)

A5.1.4. Tools/sources of information

A5.1.4.1. Regulations

A5.1.4.2. Publications, handouts

A5.1.4.3. Plans/Roadmaps

A5.1.4.4. Databases

A5.1.4.5. Formal schools/training available

A5.1.5. Standing Critical Information, indicators, and CMs

A5.1.5.1. Command

A5.1.5.2. Unit**

A5.1.5.3. Other associated organizations**

A5.1.6. How does the individual fit into the OPSEC process

A5.1.6.1. Individual responsibilities/duties

A5.1.6.2. Responsibilities/tasks of individuals office**

** Information not in HQ AFSOC training material. Developing and presenting this information is the responsibility of the unit/directorate OPSEC office

Attachment 6

AFSOC OPSEC SELF-INSPECTION CHECKLIST

	YES	NO	N/A
A6.1. Is the commander's involvement in and support of the unit OPSEC program evident? Has the commander issued an OPSEC implementing document?			
A6.2. Has an OPSEC Officer and/or NCO from all agencies specified in AFSOCI 10-1101, Para. 3.5, been appointed, in writing, to act as the focal point for all OPSEC matters?			
A6.3. Has the unit OPSEC Officer/NCO attended an OPSEC practitioner's course or program manager's course? If not, has one been scheduled through the AFSOC Program Manager?			
A6.4. Are the units' OPSEC Officers/NCOs knowledgeable about OPSEC concepts, procedures, and objectives?			
A6.5. Are unit personnel aware of the identities of the unit OPSEC Officers/NCOs?			
A6.6. Have the names of the OPSEC Officers/NCOs been forwarded to the appropriate HQ?			
A6.7. Does the local OPSEC program ensure the active participation and involvement of the entire staff or unit?			
A6.8. Does the unit have an effective OPSEC training program? Does the unit update its Critical Information annually?			
A6.9. Is the unit complying with annual OPSEC training requirements identified in AFSOCI 10-1101, para. 3.2.5.3? Are all personnel receiving training? Is it documented?			
A6.10. Does the unit develop its own training information, such as Critical Information, Indicators, countermeasures, unit responsibilities, and reminders?			
A6.11. Are personnel aware of the OPSEC threat from various intelligence collection methods?			
A6.12. Do unit personnel clearly understand the interrelationship of COMSEC, OPSEC, physical security, and information security?			
A6.13. Does the unit have AFSOCI 10-1101 or other applicable directives, which define unit OPSEC program requirements, responsibilities, and procedures?			
A6.14. Does the unit have on hand the OPSEC publications listed in AFSOCI 10-1101, Attachment 1? (this does not apply to directorates)			
	YES	NO	N/A

A6.15. Does each PLAN or OPORD contain a complete Annex L, to include a list of Critical Information, prior to publication to ensure OPSEC guidelines have been followed?			
A6.16. Are all members aware of OPSEC considerations/responsibilities as related to the planning process? Is the OPSEC process started at the very beginning of planning?			
A6.17. Is OPSEC a graded item on all formal unit inspections?			
A6.18. Are published OPSEC surveys and after action reports reviewed for possible application of findings or "lessons learned" to local on going or planned activities?			
A6.19. Has the need for an OPSEC survey been determined? If so, has one been conducted? If not, scheduled or requested?			
A6.20. Have actions been taken on recommendations to correct weaknesses or deficiencies noted in the OPSEC survey?			
A6.21. Does unit OPSEC Officer/NCO participate in Semi-annual OPSEC Meeting?			
A6.22. Do they report deficiencies/improvement opportunities at Semi-annual Meetings?			
A6.23. Do unit OPSEC Officers/NCOs nominate activities for OPSEC surveys at these meetings?			
A6.24. Is information from the Semi-annual Meetings passed on to unit personnel and subordinate units?			
A6.25. Has unit reported on the status of their program, annually, at the COMAFSOC hosted Semi-annual OPSEC Meeting?			
A6.26 Does the AFSOC program manager publish an annual report IAW AFSOCI 10-1101, Para. 3.1.6?			

Attachment 7

ANNUAL OPSEC STATUS REPORT FORMAT

A7.1. OPSEC Point of Contact

Unit name and office of primary responsibility
Name and grade of the OPSEC program manager
Mailing address
Message address
Telephone numbers (Secure, clear, and telefax)

A7.2. OPSEC Appraisal. The following areas must be assessed each year to determine program effectiveness:

- A7.2.1. The integration of OPSEC thinking into organizational plans and activities
- A7.2.2. How well those plans and OPSEC measures have been coordinated across organizational and functional lines
- A7.2.3. Training and education
- A7.2.4. Operations and exercises
- A7.2.5. Survey efforts
- A7.2.6. OPSEC program manager's status
- A7.2.7. Funding support
- A7.2.8. The effectiveness of support from intelligence and counterintelligence organizations
- A7.2.9. The areas where support or assistance is needed which is beyond the program manager's ability to acquire.

A7.3. Nominations for national OPSEC awards for each of the following categories:

- A7.3.1. Individual Achievement Award
- A7.3.2. Organizational Achievement Award
- A7.3.3. Audio-Visual Achievement Award

Attachment 8**FLOW DESCRIPTION FOR CONTINGENCY OPERATIONS****A8.1. HHQ Tasking to AFSOC**

- CRITICAL INFORMATION LIST (CIL) included?
 - No: AFSOC/DOS request CIL from tasker
 - Tasker responds with CIL?
 - No: Request CIL through OPSEC POC chain:
(AFSOC-USSOCOM-supported CINC-supported Unit)
 - Yes: Use
 - Yes: AFSOC/DOS use as basis for own CIL

A8.2. AFSOC/DOS search OPSEC database/JULLS for similar OPS

- Search positive?
 - No: Use supported organization CIL and AFSOCI 10-1101CIL (Atch 4) as basis for initial AFSOC CIL. Critical Information Component Manual is a useful tool to determine CIL.
 - Yes: Use with supported organization CIL to develop initial AFSOC CIL.

A8.3. AFSOC/DOS provide initial AFSOC CIL to functional area and subordinate unit planners to develop their CIL. List of CIL with associated indicators returned to AFSOC/DOS for compilation.

A8.4. AFSOC/DOS provides compiled AFSOC CIL w/indicators to OSI and AFSOC/IN for detailed and specific THREAT ASSESSMENT (what does he already know and how does he know it?). Assessment provided to AFSOC/DOS.

A8.5. AFSOC/DOS and subordinate unit OPSEC officers conduct VULNERABILITY ANALYSIS with functional area planners.

- Survey required (no information in OPSEC database, new; threat, tactics, participants)and time available?
 - No to either: Conduct Assessment (minimum participants DOS/IN/LG/SC)
 - Yes to both: Conduct survey IAW Joint Pub 3-54 Appendix E and JCS OPSEC Survey Guide, or National Cryptological School Guide to Performing OPSEC Assessments.
- Evaluate each CIL item and associated indicators
 - Does threat have capacity to Acquire CIL information? Is he in place to acquire it? And does he have the indicators to begin collection on it?
 - No to any: Move to next item
 - Yes to all: Identify for risk assessment

A8.6. AFSOC/DOS conducts RISK ASSESSMENT with functional area and, subordinate unit planners. Close coordination with supporting and supported unit planners recommended during this step.

- Prioritize risks
- Determine possible countermeasures for each risk
- Assess each countermeasure (CM)
 - Does vulnerability justify CM cost?
 - No: Drop from list.
 - Yes: Determine if all CM are questionable or not acceptable, present to AFSOC/CC for decision to risk exploitation by threat. Inform supported organization of risk.

A8.7. AFSOC/DOS disseminates selected countermeasures to: Supported HQ, Supporting organizations, Subordinate units, and AFSOC functional managers, who IMPLEMENT CM.

A8.8. AFSOC/DOXP documents OPSEC plan in ANNEX L of the AFSOC EXPLAN or OPORD. Subordinate units include OPSEC plan in their supporting plan or FRAGORD.

A8.9. Review and update OPSEC plan as the situation changes.

Attachment 9

FLOW DESCRIPTION FOR TRAINING EXERCISES

A9.1. Exercise proposal/directive to AFSOC. OPSEC for exercises must address both scenario and real world critical information.

- Is exercising OPSEC process an objective?
 - No: Continue with this flow description to protect real world critical information, which could be revealed by the exercise.
 - Yes: OPR/DOXE use flow description for contingency operations (substitute DOXE for DOS) during exercise planning conference in addition to continuing with this flow description.
- Is exercise HHQ directed?
 - No: AFSOC/DOXE determine OPR/level for OPSEC coordination (AFSOC, Group, Squadron). OPR/DOXE will develop initial CIL (see step 2).
 - Yes: Is CRITICAL INFORMATION LIST (CIL) included?
 - No: AFSOC/DOXE request CIL from supported organizations.
 - Supported organization responds with CIL?
 - No: Request CIL through OPSEC POC chain: (SQ-WING-AFSOC-USSOCOM-supported CINC-supported Unit).
 - Yes: Use
 - Yes: AFSOC/DOXE use as basis for own CIL

A9.2. OPR/DOXE search OPSEC database/JULLS for similar exercises

- Search positive?
 - No: Use supported organization's CIL and/or CIL from OPLAN/CONPLAN/EXPLAN being exercised plus AFSOCI 10-1101CIL (Atch 4) as basis for initial CIL. Critical Information Component Manual is a useful tool to determine CIL. Contact AFSOC/DO for command input.
 - Yes: Use with CIL from supported PLANs/organizations to develop initial CIL.

A9.3. OPR/DOXE provide initial CIL to functional area and subordinate unit planners to develop their CIL. List of CIL with associated indicators returned to OPR/DOXE for compilation.

A9.4. OPR/DOXE provides compiled AFSOC CIL W/indicators to OSI and OPR/IN for detailed and specific THREAT ASSESSMENT (what does he already know and how does he know it?). Assessment provided to OPR/DOXE.

A9.5. OPR/DOXE and subordinate unit OPSEC officers conduct VULNERABILITY ANALYSIS with functional area planners.

- Survey required (no information in OPSEC database, new PLAN being exercised, change of; threat, tactics, participants)?
 - No: Conduct Assessment (minimum participants DOXE/IN/LG/SC)
 - Yes: Conduct survey IAW Joint Pub 3-54 Appendix E and JCS OPSEC Survey Guide, or National Cryptological School Guide to Performing OPSEC Assessments.
- Evaluate each CIL item and associated indicators
 - Does threat have capacity to Acquire CIL information? Is he in place to acquire it? And does he have the indicators to begin collection on it?
 - No to any: Move to next item
 - Yes to all: Identify for risk assessment

A9.6. OPR/DOXE conducts RISK ASSESSMENT with functional area and, subordinate unit planners. Close coordination with supporting and supported unit planners recommended during this step.

- Prioritize risks
- Determine possible countermeasures for each risk
- Assess each countermeasure (CM)
 - Does vulnerability justify CM cost?
 - No: Drop from list. If CM is questionable or not acceptable, present to AFSOC/CC, through OPSEC program chain, for decision to risk exploitation by threat. Inform supported organization of risk.
 - Yes: Determine if it is the best CM

A9.7. OPR/DOXE disseminates selected CMs to exercise participants, (HHQ, Supported HQ, Supporting organizations, OPR/DOXE disseminates selected CMs to exercise participants, (HHQ, supported HQ, supporting organizations, subordinate units, and functional managers of OPR's unit), who IMPLEMENT CMs.

A9.8. OPSEC critical information and countermeasures will be briefed to participants and affected supporting organizations by their respective OPSEC officers, and will be included in the mass exercise/deployment briefing. OPR/DOXE should ensure the information is also included in exercise directive and aircrew flimsy. Both exercise scenario and real world OPSEC will be briefed and clearly identified as one or the other.

A9.9. Review and update OPSEC plan as the situation changes.

Attachment 10**FLOW DESCRIPTION FOR CURRENT OPERATIONS
TO INCLUDE SORTS AND DEPLOYMENT REPORTING**

This flow description will deal only with routine operations and reporting. As these are recurring operations, the full five step OPSEC process need only to be accomplished once, then updated as required by changes to the norm.

A10.1. AFSOC or unit directed operations?

- No: AFSOC/DOO request CIL (if any) and countermeasures (CMs) from supported unit. Use as appropriate in conjunction with AFSOC CIL and CMs.
- Yes: Go to step 2

A10.2. Unit/DOO search AFSOC OPSEC database for similar OPS

- Search positive?
 - No: Accomplish full five step OPSEC process
 - Yes: Adhere to the identified CRITICAL INFORMATION LIST (CIL) and CMs. Go to step 7

A10.3. Unit/DOO provide initial CIL (from AFSOCI 10-1101 and supported unit inputs) to functional area and subordinate unit planners to develop their CIL. Critical Information Component Manual is a useful tool to determine CIL. List of CIL with associated indicators returned to unit/DOO.

A10.4. Unit/DOO provides compiled CIL W/indicators to Unit/IN and OSI for detailed and specific THREAT ASSESSMENT (what does he already know and how does he know it?). Assessment provided to Unit/DOO.

A10.5. Unit/DOO and subordinate unit OPSEC officers conduct VULNERABILITY ANALYSIS with functional area planners.

- Survey required (no information in OPSEC database, threat significant)?
 - No: Conduct Assessment (minimum participants DO/IN/LG/SC)
 - Yes: Conduct survey IAW Joint Pub 3-54 Appendix E and JCS OPSEC Survey Guide, or National Cryptological School Guide to Performing OPSEC Assessments.
- Evaluate each CIL item and associated indicators
 - Does threat have capacity to Acquire CIL information? Is he in place to acquire it? And does he have the indicators to begin collection on it?
 - No to any: Move to next item
 - Yes to all: Identify for risk assessment

A10.6. Unit/DOO conducts RISK ASSESSMENT with functional area and, subordinate unit planners. Close coordination with supporting and supported unit planners recommended during this step.

- Prioritize risks
- Determine possible countermeasures for each risk
- Assess each CM
 - Does vulnerability justify CM cost?
 - Yes: Determine if it is the best CM
 - No: Drop from list. If all CM are questionable or not acceptable, present to AFSOC/CC, through OPSEC chain, for decision to risk exploitation by threat.

A10.7. Unit/DOO disseminates selected countermeasures to unit individuals and OPSEC POCs of supporting/supported units who IMPLEMENT CM.

A10.8. Unit/DOO documents OPSEC plan in AFSOC OPSEC database. OPSEC CMs for routine and recurring operations and reports will be coordinated with the AFSOC OPSEC program manager, at the semi-annual OPSEC meeting, for inclusion in the annual OPSEC training program.

A10.9. Review and update OPSEC plan as the situation changes.

Attachment 11**FLOW DESCRIPTION FOR FORCE AND DOCTRINE DEVELOPMENT,
PROGRAMMING AND DEFENSE ACQUISITION SYSTEMS PROCESS**

This effort should concentrate on protecting the existence of critical limitations until they are corrected, or significant new tactics/capabilities for as long as possible.

A11.1 Requirement or shortfall identified to AFSOC.

- External source?
 - No: Go to step 2
 - Yes: AFSOC/XP request CRITICAL INFORMATION LIST (CIL) from source. Use as appropriate in conjunction with AFSOC developed CIL and countermeasures (CMs).

A11.2 AFSOC/XP search OPSEC database/JULLS for similar situation

- Search positive?
 - No: Use supported organization CIL and AFSOCI 10-1101 CIL (Atch 4) as basis for initial AFSOC CIL. Critical Information Component Manual is a useful tool to determine CIL.
 - Yes: Use with external source CIL to develop initial AFSOC CIL.

A11.3 AFSOC/XP provide initial AFSOC CIL to AFSOC/DO/FM/and other offices and units involved in the process to develop their own CIL. List of CIL with associated indicators returned to AFSOC/XP for compilation.

A11.4 AFSOC/XP provides compiled AFSOC CIL W/indicators to AFSOC/IN and OSI for detailed and specific THREAT ASSESSMENT (what does he already know and how does he know it?). Assessment provided to AFSOC/XP.

A11.5 AFSOC/XP officer conducts VULNERABILITY ANALYSIS with offices/units involved in force and doctrine development and the MAP and Weapon System Roadmap processes.

- Survey required (no information in OPSEC database, or significantly new capability or limitations)?
 - No: Conduct Assessment (minimum participants XP/FM/DO/IN/contractor)
 - Yes: Conduct survey IAW Joint Pub 3-54 Appendix E and JCS OPSEC Survey Guide, or National Cryptological School Guide to Performing OPSEC Assessments.
- Evaluate each CIL item and associated indicators
 - Does threat have capacity to Acquire CIL information? Is he in place to acquire it? And does he have the indicators to begin collection on it?
 - No to any: Move to next item
 - Yes to all: Identify for risk assessment

A11.6. AFSOC/XP conducts RISK ASSESSMENT with contributing functional area offices and units.

- Prioritize risks
- Determine possible CMs for each risk
- Assess each CM
 - Does vulnerability justify CM cost?
 - No: Drop from list.
 - Yes: Determine if it is the best CM. If all CM are questionable or not acceptable, present to AFSOC/CC for decision to risk exploitation by threat. Inform USSOCOM-J5 of risk.

A11.7. AFSOC/XP disseminates selected CMs to all involved organizations OPSEC officers (Supported HQ, Supporting organizations to include contractors, Subordinate units, and AFSOC functional managers), who IMPLEMENT CMs.

A11.8. AFSOC/XP documents OPSEC plan in AFSOC OPSEC database and in development and implementing documents.

A11.9. Review and update OPSEC plan as the situation changes.

Attachment 12**FLOW DESCRIPTION FOR RESOURCE
BUDGETING/ALLOCATION PROCESS**

This effort should concentrate on protecting details of future projects/structure/operations revealed during the process, and the existence of critical limitations used for justification of funding.

A12.1. Requirement or shortfall identified to AFSOC

- External source?
 - No: Go to step 2
 - Yes: AFSOC/FM request EEFI/CRITICAL INFORMATION LIST (CIL) from source. Use as appropriate in conjunction with AFSOC developed CIL and countermeasures (CMs).

A12.2. AFSOC/FM search OPSEC database/JULLS for similar situation

- Search positive?
 - No: Use supported organizations CIL (if any) and AFSOCI 10-1101 CIL (Atch 4) as basis for initial AFSOC CIL. Critical Information Component Manual is a useful tool to determine CIL.
 - Yes: Use with external source CIL to develop initial AFSOC CIL.

A12.3. AFSOC/FM provide initial AFSOC CIL to AFSOC/DO/XP/and other offices and units involved in the process to develop their own CIL. List of CIL with associated indicators returned to AFSOC/FM for compilation.

A12.4. AFSOC/FM provides compiled AFSOC CIL w/indicators to AFSOC/IN and OSI for detailed and specific THREAT ASSESSMENT (what does he already know and how does he know it?). Assessment provided to AFSOC/FM.

A12.5. AFSOC/FM OPSEC officer conducts VULNERABILITY ANALYSIS with offices/units involved in force and doctrine development.

- Survey required (no information in OPSEC database, or process may reveal significantly new capability or limitations)?
 - No: Conduct Assessment (minimum participants FM/XP/DO/IN)
 - Yes: Conduct survey IAW Joint Pub 3-54 Appendix E and JCS OPSEC Survey Guide, or National Cryptological School Guide to Performing OPSEC Assessments.
- Evaluate each CIL item and associated indicators
 - Does threat have capacity to acquire CIL information? Is he in place to acquire it? And does he have the indicators to begin collection on it?
 - No to any: Move to next item
 - Yes to all: Identify for risk assessment

A12.6. AFSOC/FM conducts RISK ASSESSMENT with contributing functional area offices and units.

- Prioritize risks
- Determine possible countermeasures for each risk
- Assess each CM
 - Does vulnerability justify CM cost?
 - No: Drop from list.
 - Yes: Determine if it is the best CM. If all CM are questionable or not acceptable, present to AFSOC/CC for decision to risk exploitation by threat.

A12.7. AFSOC/FM disseminates selected CMs to all involved organizations OPSEC officers (USSOCOM, Supporting organizations, Subordinate units, and AFSOC functional managers), who IMPLEMENT CMs.

A12.8. AFSOC/FM documents OPSEC plan in AFSOC OPSEC database and in programming and allocation documentation.

A12.9. Review and update OPSEC plan as the situation changes.

Attachment 13

GENERIC CONTINUITY FOLDER

A15.1. Cover	Classify according to overall content
A15.2. Table of Contents	A/R
A15.3. Letter of Appointment	Letter signed by commander or director
A15.4. Mission Statement, Duties and Responsibilities, Background Information	State what you and your program are out to accomplish
A15.5. Critical Information (CI), Indicators and Countermeasures (CM)	List the CI your organization is trying to protect, actual or potential indicators, and applicable CM
A15.6. Review Log	Everyone who looks at your books signs/dates
A15.7. OPSEC Policy Guidance Letters	A/R
A15.8. OPSEC Regulations/Directives	AFSOCI 10-1101 and most often used regulations
A15.9. Inspections	Maintained until superseded
A15.10. Training Records	Maintain until superseded
A15.11. OPSEC Working Groups	Charter, members, contact numbers, minutes
A15.12. OPSEC Points of Contact	Update regularly
A15.13. Annual OPSEC Report	A/R
A15.14. OPSEC Program Manager's Course Guide and other Reference Guides	Course guides provided through attendance at an OPSEC program manager's course
A15.15. Miscellaneous	OPSEC correspondence and other applicable material
A15.16. Installation Multidiscipline Threat Information (or the location where this information is available)	Threat information obtained through Intelligence or OSI (may be stored separately due to classification level)
A15.17. OPSEC Surveys or Appraisals	Maintain for five years or until superseded
A15.18. OPSEC Training materials, Recurring Periodicals	Briefings, pamphlets, handouts, AFIWC OPSEC Update, IOSS OPSEC Indicator, listing of video tapes available